МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ТЕОРИИ УПРАВЛЕНИЯ СЛОЖНЫХ ПРОЦЕССОВ

КЛАССИФИКАЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ

С.П. Еременко, кандидат технических наук, доцент;
А.И. Сапелкин;
С.Б. Хитов.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены нормативно-методические основы классификации угроз информационной безопасности, связанных с применением вредоносных программ в отношении информационных систем органов управления МЧС России. Выделены угрозы воздействия на информационные системы отдельных типов вредоносных программ.

Ключевые слова: информационная безопасность, вредоносная программа, компьютерный вирус, DOS-атаки, угрозы, классификация, признаки вредоносных программ, троянская программа, сетевые черви, полиморфные вирусы

CLASSIFICATION OF MALWARE

S.P. Eremenko; A.I. Sapelkin; S.B. Khitov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

Legal and methodological bases for the classification of information security threats associated with the use of malicious programs for information systems managerial bodies of EMERCOM of Russia are considered by the authors. The threats of separate types of malware are allocated.

Keywords: information security, malware, computer virus, DOS attacks, threats, classification, feature of malware, trojan, worms, polymorphic viruses

Современное состояние МЧС России характеризуется повышением уровня информатизации в деятельности органов управления на всех уровнях. Качество принимаемых должностными лицами управленческих решений напрямую зависит от эффективности использования информационно-телекоммуникационной инфраструктуры, включающей в себя информационные системы (ИС) и ресурсы, а также средства, обеспечивающие их функционирование, взаимодействие между собой, населением и организациями.

Концентрация больших объемов информации, циркулирующих в ИС органов управления МЧС России, ведет к увеличению вероятности утечки конфиденциальных сведений, а значит, и к необходимости принятия мер по обеспечению безопасности информации.

При этом нарушение целостности, доступности и актуальности информации, используемой в процессах принятия решения, ставит под угрозу возможность выполнения возложенных на МЧС России функциональных задач [1].

Защита информации в МЧС России является проблемой комплексной [2]. Выполнение мероприятий в рамках ее решения невозможно без проведения оценки и анализа угроз информационной безопасности (угроз). Кроме того, определение угроз является одним из требований нормативных методических документов, регулирующих вопросы обеспечения информационной безопасности Российской Федерации [3].

Существует множество подходов к классификации угроз. В работе [4] авторами представлена обобщенная классификация угроз для распределенных вычислительных сетей, являющихся материальной (технической) основой реализации целого ряда ИС МЧС России. Классификационными признаками выделены источник угрозы, ее характер, вид воздействия и направленность угрозы.

Согласно данной классификации можно выделить технологические угрозы программного (логического) воздействия, реализуемые как внутренними, так и внешними локальными либо удаленными нарушителями.

ГОСТ Р 51275–2006 [5] выделяет одним из субъективных факторов (а совокупность условий и факторов, создающих потенциальную или реально существующую опасность, нарушения безопасности информации можно рассматривать как угрозу [6]), воздействующих на безопасность защищаемой информации – несанкционированный доступ (НСД) к информации путем применения вирусов или другого вредоносного программного кода.

Причем данный фактор может быть как внешним, так и внутренним по отношению к объекту информатизации.

К вредоносному программному коду или вредоносной программе относят программу, предназначенную для осуществления НСД к информации и (или) воздействия на информацию или ресурсы ИС [6].

Специальные нормативные документы одного из отечественных регуляторов в области информационной безопасности – Федеральной службы по техническому и экспертному контролю (ФСТЭК) России относят к источникам угроз НСД носителей вредоносных программ и определяют такие угрозы как угрозы программно-математического воздействия [7].

В целях обеспечения безопасности ИС необходимо выявить и классифицировать эти угрозы. Это позволит для каждой вредоносной программы (ВП) разработать свои способы и методы обнаружения, ликвидации и предупреждения.

Почти каждая ВП имеет свое предназначение и создана для достижения определенной цели как по проникновению, так и по нанесению вреда информационной системе.

ВП – программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной ИС [5].

В настоящей статье компьютерные вирусы, компьютерные атаки, сетевые атаки и программные воздействия будут называться ВП.

Дадим классификацию ВП по наиболее выраженным признакам, опираясь на нормативные документы [7] одного из отечественных регуляторов в области информационной безопасности – ФСТЭК России, в которых частично отображается классификация программных вирусов и сетевых червей.

Классификацию ВП дадим по следующим признакам.

1. По особенностям алгоритма работы и сложности кода.

Под троянской программой будем подразумевать ВП, которую используют киберпреступники в целях скрытого сбора конфиденциальной информации, модификации и различных деструктивных действий, приводящих к нарушению работоспособности ЭВМ, утечки данных.

Под логической бомбой будем подразумевать разновидность троянской программы, активирующейся в заданное время.

Под понятием кейлогер будем понимать программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д.

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными [7].

Программы-маскировщики – утилиты, используемые для сокрытия вредоносной активности. Они маскируют ВП, чтобы избежать их обнаружения антивирусными программами [8].

Бэкдор – ВП, дефект алгоритма которого намеренно встраивается в неё разработчиком и позволяет получить тайный доступ к данным или удалённому управлению компьютером.

Анти-антивирус – ВП, объектом нападения которой являются антивирусные программы.

Антивирусная ВП – ВП, объектом нападения которой являются другие различные компьютерные вирусы.

Простейшие вирусы – компьютерные вирусы, которые изменяют содержимое файлов и секторов диска.

Стелс-вирусы – компьютерные вирусы, частично или полностью скрывающие свое присутствие в компьютерной системе.

Полиморфные вирусы – компьютерные вирусы, способные изменять собственный код методами различного шифрования или использованием искусственного интеллекта.

Руткиты – набор программных средств, предназначенных для сокрытия присутствия других ВП, а также для обеспечения маскировки объектов контроля и сбора данных.

Практически любая ВП оказывает деструктивное воздействие на ЭВМ и определяется степенью последствий. Поэтому введем второй классификационный признак – деструктивные возможности.

2. По деструктивным возможностям ВП делятся на [7]:

– безвредные, то есть не влияющие на производительность и функционирование компьютера;

– неопасные, то есть способствуют уменьшению свободной памяти и их проявление сопровождается графическими и звуковыми эффектами;

– опасные, то есть ведущие к серьезным сбоям в работе компьютера;

– очень опасные, то есть ведущие к изменению, модификации, утрате и уничтожению информации.

Вооруженные Силы Российской Федерации, МЧС России, МВД России, ФСБ России, средства массовой информации, а также другие государственные, политические, образовательные и научные организации, предприятия различного рода, используют в своей деятельности интернет. Масштаб его распространения носит глобальный характер. В тоже время незащищённость интернет-технологий информационной сети способствует мгновенному распространению ВП, что делает её уязвимой. В соответствии с этим выделим следующий признак – по использованию интернет технологий и дадим им ряд определений.

3. По использованию интернет технологий разделим ВП на следующие типы:

Трояны загрузчики – троянские программы, которые скрытно, несанкционированно загружаются из сети.

Программное обеспечение фишинга – производят почтовую рассылку с целью получения от пользователя конфиденциальной информации (в основном финансового характера).

Программы-рекламы – вредоносные программные модули, которые без уведомления пользователя включены в состав программ с целью показа рекламных объявлений.

Флуд – сетевая (компьютерная) атака, связанная с большим количеством сформированных в неправильном формате запросов к компьютерной системе с целью получения отказа в ней.

Программы-шпионы – ВП, которые незаметно проникают на ЭВМ с целью слежения и сбора конфиденциальной информации об организации или пользователе без их согласия.

Клавиатурные шпионы – вредоносные программы, предназначенные для скрытной записи информации о нажимаемых пользователем клавишах и отсылающие эту информацию киберпреступнику.

Сетевые черви – ВП, распространяемые по компьютерной сети, используя различные уязвимости ЭВМ для несанкционированного доступа к системе с дальнейшим самораспространением.

Данные классы червей приведены в методической документации ФСТЭК России, но отсутствует понятийный аппарат. Условно введём его:

– P2P-черви – черви, распространяющиеся при помощи пиринговых файл обменных сетей;

– IRC-черви – черви, распространяющиеся по каналам IRC;

– почтовые черви – черви, распространяющиеся в формате сообщений электронной почты;

– IM-черви – черви, использующие для распространения системы мгновенного обмена сообщениями.

Ботнет представляет собой зараженную ВП (ботами) компьютерную сеть и позволяет киберпреступникам удаленно управлять ей с целью DOS-атак, рассылки спама, сбора конфиденциальной информации, перебора паролей на удалённой системе и т.д.

Под DOS-атакой будем понимать атаку киберпреступника на информационную сеть с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам либо этот доступ затруднён.

Выделим наиболее распространенные типы DOS-атак:

– атака на насыщения полосы пропускания канала связи;

– атака, приводящая к недостатку системных ресурсов;

– атака, использующая ошибки программы;

– атака на DNS–сервера;

– комбинированные DOS-атаки или другие (другими DOS-атаками будем называть те атаки, у которых модифицируются алгоритмы и приёмы воздействия).

4. Распространяемые по сети.

Для выявления границ заражения ВП условно разделим информационную сеть на три вида: внутреннюю, внешнюю и специализированную. Сопоставим эту градацию с общими признаками сети следующим образом:

– внешняя – глобальная вычислительная сеть;

– внутренняя – локальная вычислительная сеть;

– специализированная – ведомственная вычислительная сеть.

Глобальная вычислительная сеть – вычислительная сеть, охватывающая достаточно большую территорию. Под достаточно большой территорией понимают регион, страну или несколько стран [9].

Локальная вычислительная сеть – вычислительная сеть, охватывающая небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных. Под небольшой территорией понимают здание, предприятие, учреждение [9].

Под ведомственной вычислительной сетью будем понимать компьютерную сеть, создаваемую для производственных и специальных потребностей органов государственной власти.

Главным элементом информационной сети является ЭВМ. ЭВМ включает в себя аппаратные и программные части. Процесс выполнения различных операций требует загрузки операционной системы и программных продуктов различного уровня, в том числе и ВП, поэтому выделим следующий признак.

5. Вирусы, активирующиеся при загрузке системы.

Link-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» операционную систему выполнить свой код [7].

К категории «компаньон» относятся вирусы, не изменяющие заражаемые файлы. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, то есть вирус [7].

Файловые черви – при размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем [7].

Под резидентными вирусами будем понимать компьютерные вирусы, которые при инфицировании ЭВМ загружаются в оперативную память и перехватывают функции операционной системы к объектам заражения и внедряется в них.

Под полурезидентными вирусами будем подразумевать компьютерные вирусы, загружаемые и выполняемые совместно с невредоносной программой.

Под нерезидентными (транзитными) вирусами будем понимать компьютерные вирусы, не заражающие оперативную память ЭВМ, которые выполняются в момент запуска зараженной программы

Перезаписываемые вирусы – компьютерные вирусы, которые стирают (перезаписывают) информацию в зараженных файлах.

В зависимости от цели и способа воздействия на ЭВМ ВП программы имеют различную среду обитания, поэтому следующим будет признак – среда обитания.

6. По среде обитания ВП разделим на

Макровирусы являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.) [7].

Файловые, то есть внедряются в выполняемые файлы операционных систем (*.exe, *.com, *.dll, *.sys, *.bat, *.cmd).

Загрузочные, то есть внедряются в загрузочный сектор диска или в сектор, содержащий системный загрузчик диска.

Файлово-загрузочные, то есть заражающие как файлы, так и загрузочные сектора.

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию [7]:

– сетевые протоколы, то есть используют для своего распространения протоколы компьютерных сетей;

– сетевые команды, то есть используют для своего распространения команды компьютерных сетей;

– электронной почты, то есть используют для своего распространения электронную почту;

– другие сетевые сервисы, то есть используют менее популярные для своего распространения инструменты;

– flash (BIOS), то есть для своего распространения использует постоянное запоминающее устройство.

Знания об источниках угроз позволяют выявить слабые места в информационной сети органов управления МЧС России. Поэтому необходимо провести классификацию ВП по способу проникновения в систему.

7. По способу проникновения в систему:

– интернет – глобальная информационная сеть является основным источником распространения любого рода ВП [8];

– электронная почта – сообщения, поступающие в почтовый ящик пользователя, могут содержать в себе различные типы ВП;

– уязвимости в программном обеспечении. Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации [10];

– внешние носители информации. Запуская какой-либо файл, расположенный на внешнем носителе, вы можете поразить данные на вашем компьютере вирусом и, незаметно для себя, распространить вирус на диски вашего компьютера [8].

– пользователи. Доверчивые пользователи сами устанавливают безобидные на первый взгляд программы, заражая таким образом свой компьютер. Этот метод называется социальной инженерией – вирусописатели добиваются того, чтобы жертва сама установила зловредное программное обеспечение при помощи различных уловок [8].

Существующие операционные системы отличаются технологиями разработки, системой функционирования, безопасности и т.д., поэтому введем и этот признак.

8. По заражаемым операционным системам:

– Unix/Linux – несколько дистрибутивов, основанных на исходной системе Unix;

– Windows – операционные системы, разработанные корпорацией Microsoft;

– MACOS – операционная система, разработанная компанией Apple;

– MS-DOS – первая операционная система без графического интерфейса, разработанная корпорацией Microsoft.

Активация ВП прямым образом зависит от их времени функционирования.

9. По времени воздействия:

– непрерывное;

– периодическое;

– временное.

Проведенный анализ классификации ВП выявил наличие огромного количества разнообразных программ такого рода, обладающих классификационными признаками. Каждая ВП, в свою очередь, имеет разные функции, задачи и свойства. Реализация угроз безопасности информации, связанных с применением ВП, может привести к нарушению всех свойств безопасности информации – конфиденциальности, доступности и целостности. При этом количество вредоносных программ растет по мере развития и усложнения программного обеспечения, а взаимодействия, приводящие к реализациям подобных угроз, имеют достаточно сложный характер. В связи с этим для исследования вопросов, связанных с разработкой комплексных систем защиты информации, широко используются модели реализации угроз, основой построения которых будет являться рассмотренная выше классификация ВП.

Литература

1. Чижиков Э.Н. Защита информации для безопасного функционирования информационных систем МЧС России // Каталог пожарной безопасности. 2013. № 1 (14). С. 16–17.

2. Еременко С.П., Хитов С.Б. Оценка результативности как важнейший аспект построения системы обеспечения информационной безопасности в системе распределенных ситуационных центров МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2016. № 2. С. 84–90.

3. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11 февр. 2013 г. № 17 // Официальный сайт ФСТЭК России.

URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 22.06.2016).

4. Иванов А.Ю., Синещук М.Ю. Классификация нарушителей и угроз безопасности автоматизированной информационной управляющей системы МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2013. № 4. С. 74–79.

5. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Стандартинформ, 2007. 7 с.

6. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. М.: Стандартинформ, 2007. 12 с.

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (утв. зам. директора ФСТЭК России 15 февр. 2008 г.). URL: http://fstec.ru/component/attachments/download/289 (дата обращения: 22.06.2016).

8. О вирусах: Основные источники проникновения угроз на компьютер. URL: http://support.kaspersky.ru/789 (дата обращения: 14.04.2016).

9. ГОСТ 24402–88. Телеобработка данных и вычислительные сети. Термины и определения. URL: http://www.wseas.us/e-library/transactions/computers/2008/25-667.pdf (дата обращения: 14.04.2016).

10. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2015. 8 с.

References

1. Chizhikov E.N. Information protection for secure functioning of information systems of EMERCOM of Russia // Directory of fire safety. 2013. № 1(14). P. 16–17.

2. Eremenko S.P., Hitov S.B. Evaluating performance as an important aspect of the construction of the system of ensuring information security in the system of distributed situational centers of EMERCOM of Russia // Vestnik S.-Petersb. un-ty of State fire service of EMERCOM of Russia. 2016. № 2. P. 84–90.

3. On approval of requirements for protection of information not constituting a secret of state, contained in state information systems: the Order of the FSTEC of Russia from 11.02.2013 № 17 // Official site of the FSTEC of Russia. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17.

4. Ivanov A.Yu., Senesouk M.Yu. Classification of intruders and security threats automated information management system of EMERCOM of Russia // Vestnik S.- Peterb. un-ty of State fire service of EMERCOM of Russia. 2013. № 4. P. 74–79.

5. GOST R 51275–2006. The protection of information. The object of Informatization. Factors affecting information. General provisions. M.: STANDARTINFORM, 2007. 7 p.

6. GOST R 50922–2006. The protection of information. Basic terms and definitions. M.: STANDARTINFORM, 2007. 12 p.

7. The basic model of threats to the security of personal data during their processing in personal data information systems (extract), approved. Deputy Director FSTEK of Russia 15.02.2008. URL: http://fstec.ru/component/attachments/download/289.

8. About viruses: the Main sources of threats penetration to the computer. URL: http://support.kaspersky.ru/789 (accessed: 14.04.2016).

9. GOST 24402–88. Teleoperate the data and the computer network. Terms and definitions. URL: http: //www.wseas.us/e-library/transactions/computers/2008/25-667.pdf. (accessed: 14.04.2016).

10. GOST R 56546–2015. The protection of information. Vulnerability of information systems. Classification of vulnerabilities of information systems. M.: STANDARTINFORM, 2015. 7 p.